

GUÍA BÁSICA DE AUTODEFENSA DIGITAL PARA CELULARES

32° ENCUENTRO NACIONAL DE MUJERES, TRANS TRAVAS Y LESBIANAS

CHACO, 2017


HACKEA TU
LUCHA

“No tengo nada que ocultar en mi teléfono” . - Pues sí, todxs tenemos cosas que ocultar o por lo menos, deberíamos.-

Moxie Marlinspike

Nuestros teléfonos no solo son ventanas abiertas en nuestras vidas, sino también en las vidas de nuestrxs amigxs, familias, compas...y cualquiera de nuestrxs contactos. Quizás se piense que no hay nada para ocultar pero no podemos asegurar lo mismo por todxs los contactos con lxs que interactuamos por vía telefónica. Proteger la información de nuestro teléfono es también proteger a nuestrxs amigxs.

Cuando hacemos una llamada telefónica o enviamos mensajes, se registran al menos la ubicación geográfica de quien llama y quien contesta, sus números de teléfono, la hora y duración de la comunicación y los números de serie de los dispositivos utilizados. De igual manera pueden ser capturados los datos de nuestras comunicaciones por medio de alguna aplicación del smartphone. En un mismo aparato se vinculan los datos del número telefónico, correo, contactos, actividad en redes sociales, SMS, fotografías, archivos, datos de GPS y a veces la sincronización con otros dispositivos.

Hay que tener en cuenta que los métodos de espionaje estatales-empresariales se han perfeccionado y que nosotrxs participamos de manera activa en la maquinaria de vigilancia. Esta maquinaria no descansa y su funcionamiento es eficiente por definición. No es restrictiva sino silenciosa, no es reactiva sino retroactiva, no es solo individual y dirigida, sino también masiva.

Estamos convencidxs de que es momento de salir de la interpasividad impuesta para tener una participación activa y critica en cuanto a las formas y los medios que elegimos al comunicarnos. La seguridad y la privacidad de nuestros datos y comunicaciones son una construcción colectiva y una práctica de cuidado.

Más allá de las herramientas que utilicemos, lo fundamental para construir una comunicación segura es afianzar las prácticas colectivas de seguridad (lo que decimos, la forma y el momento en que lo decimos)

siendo indispensable la participación y el compromiso de cada unx de nosotrxs.

Este fanzine es una guía básica para configurar nuestros celus de forma segura y un primer paso en la autodefensa digital. Lo editamos en el marco del 32° encuentro nacional de mujeres, trans, travestis y lesbianas en Chaco, primavera del 2017. Quienes lo realizamos creemos que es necesario dar discusión sobre el cuidado en relación a las comunicaciones mediadas por la tecnología digital y a las estrategias que elegimos cuando hablamos de autodefensa feminista. Esperamos sea de utilidad. Celebramos profundamente que se comparta, se intervenga, se potencie.

Octubre 2017.

Córdoba, Argentina.



TIPS DE PREVENCIÓN PARA ASEGURAR TU TELÉFONO

(con android)

¿Que información tiene un teléfono de mi?

- Historial de llamadas, mensajes de texto enviados y recibidos, información de libretas de direcciones y calendarios.
- Fotos, Videos, archivos de texto. -Mails y acceso a redes sociales. Conversaciones y grupos de Whatsapp y Telegram.
- Localización exacta mia en todo momento por medio de la red de telefonia y por medio del GPS

Es importante que estemos al tanto de la información que se almacena, tanto en forma activa como pasiva, en el teléfono, ya sea en tu tarjeta SIM o en la memoria del teléfono. Estos datos revelan tu red de contactos y tu información personal.

En primer lugar, no hay que guardar información sensible en el teléfono. Si no tenés otra opción es mejor almacenar dicha información en tarjetas de memoria externas que puedan ser fácilmente desechadas en caso necesario – ***no coloques ningún detalle en la memoria interna del teléfono.***

Quienes nos observan no necesitan saber con precisión lo que hemos dicho, pueden llegar a conclusiones solo analizando los ***metadatos*** que nuestras comunicaciones producen durante un tiempo. Hay que tener siempre presente que los métodos de control y vigilancia digital y los métodos que tenemos para defendernos están en constante cambio y actualización por lo que debemos estar siempre atentxs y adecuar nuestros hábitos siendo cuidadosxs en el manejo y circulación de nuestra información sensible, pero sobre todo comprender que la autodefensa no es algo que podamos hacer individualmente sino que es una construcción colectiva.

1- Bloquea tu teléfono

¿Qué significa?

Cambiar tus preferencias así el celular se bloquea después de un tiempo o cuando aprietes el botón de apagado y no se acceda a tu contenido rápidamente sin conocer el código.

¿Cómo hacerlo?

Acceder a Ajustes o Configuración → Seguridad → Bloqueo de pantalla

Podes elegir entre:

- PATRÓN: será un determinado movimiento que tendrás que hacer con el dedo en la pantalla.
- PIN: un número de 4 cifras
- CONTRASEÑA: letras y números elegidos.

Si olvidas el código de bloqueo podes desbloquearlo con tu cuenta de gmail o resetear el móvil totalmente.

2- Encriptá tu celular

¿Qué significa encriptar o cifrar el teléfono?

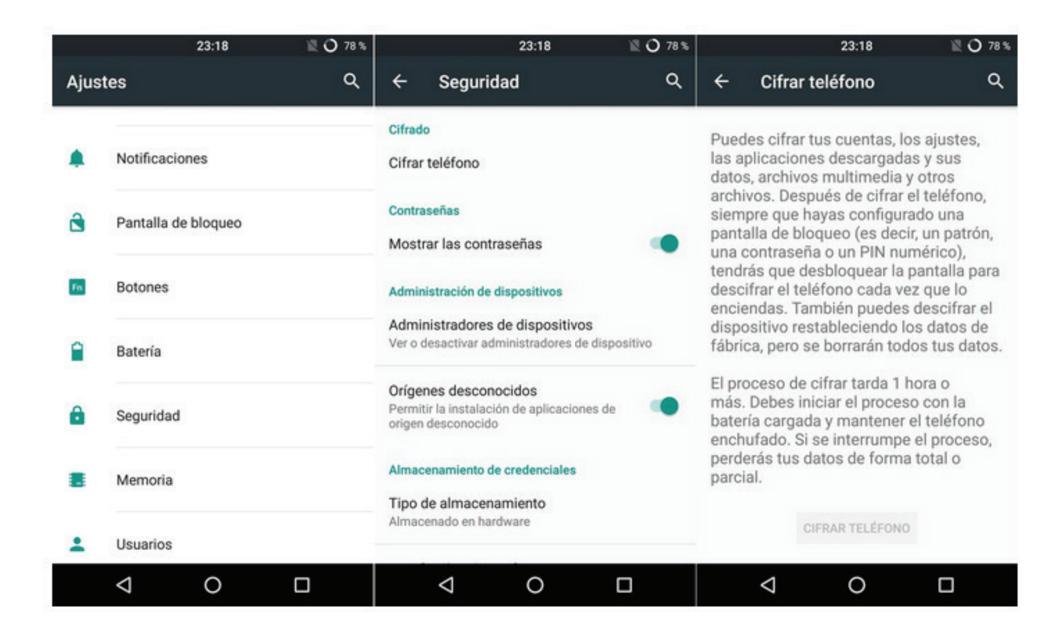
Es hacer que ***la información que hay dentro de tu dispositivo sea mucho menos accesible*** de lo habitual. Esto se consigue haciendo que para llegar a cierta información que tengas almacenada tengas que introducir una contraseña, de forma que si el teléfono cae en otras manos, tengas cierta tranquilidad de que tus datos no estarán tan expuestos. Una vez cifrado tu celular, la música, vídeos, fotos y datos de aplicaciones sólo serán accesibles si introduces la ***contraseña o el código PIN*** que has configurado antes de iniciar el proceso.

¿Cómo hacerlo?

En todas las versiones de Android el proceso es muy similar, puede variar la ruta en la que se encuentre esta opción, pero será muy similar independientemente de la marca de tu móvil.

Pasos:

1. Enchufar el teléfono, el proceso puede durar una hora.
2. Tener configurado un método de desbloqueo de la pantalla: tiene que ser pin o contraseña, no puede ser facial, ni patron, ni el simple deslizamiento.
3. Acceder a Ajustes o Configuración → Seguridad → Cifrar teléfono



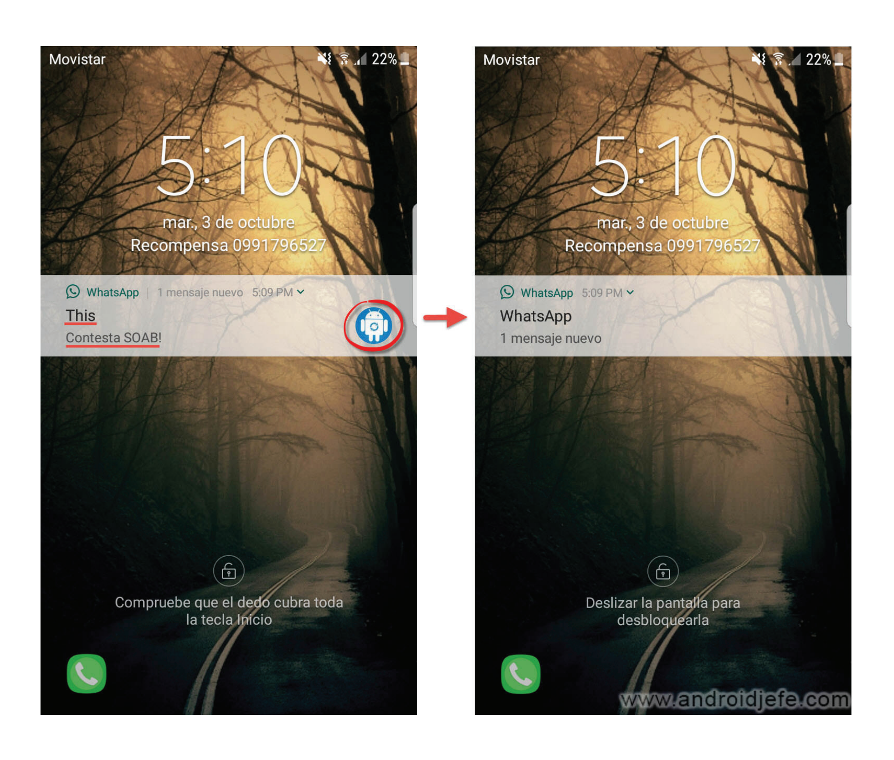
4. Confirmar el PIN o contraseña y esperar a que el proceso termine, que puede tardar una hora aproximadamente, y no interrumpirlo. En caso de que el teléfono tenga una tarjeta microSD, los datos que contiene también serán cifrados, por lo que si la pasas a otro celular no podrás usarlos a no ser que primero lo desencriptes.

3- Ocultá tus mensajes

Previene que las aplicaciones de mensajería, como whatsapp o telegram, muestren el mensaje completo al recibir uno nuevo cuando tu teléfono esta bloqueado.

¿Cómo lo hago en whatsapp?

1. Ajustes o Configuración
2. Aplicaciones
3. WhatsApp
4. Notificaciones
5. Desactivar la opción "Permitir notificaciones" o "Permitir dar un vistazo" (y activar alguna opción que no muestre los mensajes en la pantalla principal como "Ocultar contenido confidencial" o "Bloquear Todos").



¿Cómo lo hago en telegram?

1. Abrir Telegram
2. Configuración
3. Ajustes
4. Notificaciones y sonidos
5. Desactivar "Vista previa del mensaje"

4- Utilizar contraseñas fuertes

Utiliza frases de paso, autenticación de dos pasos y contraseñas fuertes y diferentes para diferentes cuentas.

- FRASES DE PASO : Una frase que represente algo para nosotrxs, que sea larga, que incluya números, caracteres especiales y tanto mayúsculas como minúsculas. Ejemplos: una forma de generar una contraseña sencilla de recordar y, aun así larga sería algo por el estilo: "MiCuentaDe_Twitter_SeCreoEn2011". Otra posibilidad es recurrir a algo mas familiar "MiPrimerMovilFu€UnNokia3310" o "ElPisoEnElQueVivoEsUn3ero!".

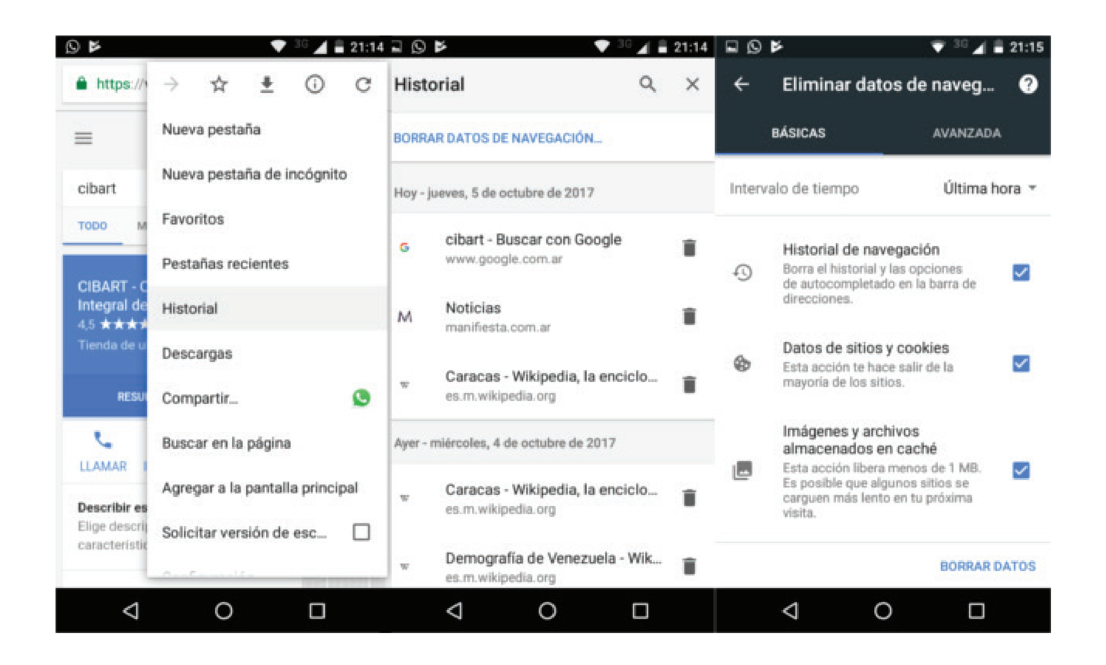
- AUTENTICACIÓN DE DOS PASOS: una vez habilitada, la aplicación nos pedirá la contraseña mas un método alternativo de autenticación, típicamente un código único enviado por SMS. Esto ofrece mayor protección a tu cuenta al demandar la comprobación de identidad por más de un método. Esto significa que, aunque alguien obtenga acceso a su contraseña primaria, no podrá invadir su cuenta a no ser que también posea su teléfono móvil o otro medio secundario de autenticación.

5- Borrar el historial de navegación

Borrar frecuentemente el historial de navegación de los buscadores desde sus ajustes.

¿Cómo lo hago en Chrome?

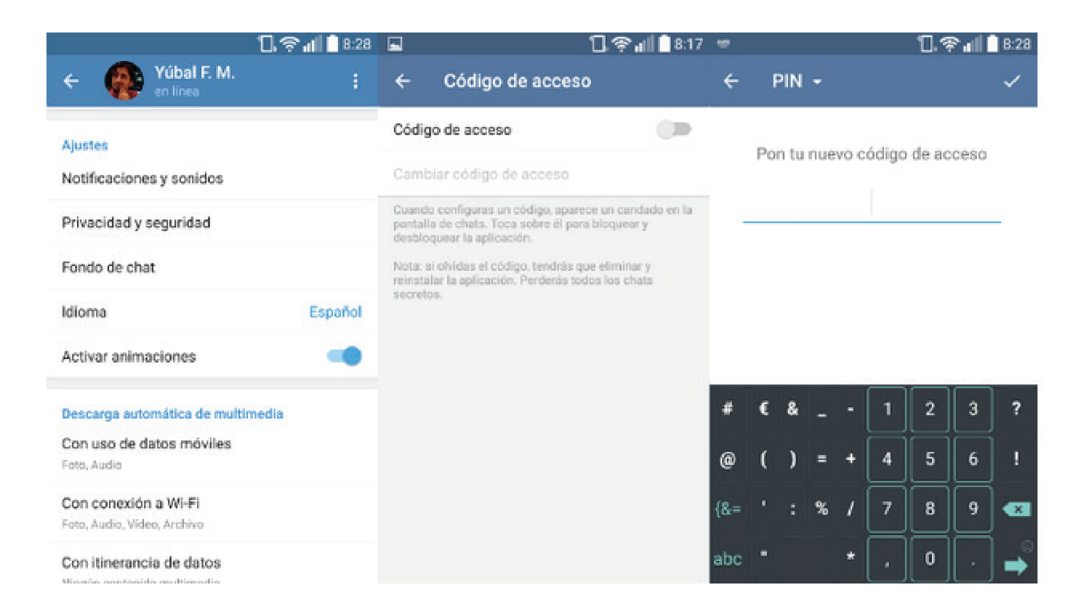
1. Abrir chrome
2. Configuración
3. Historial
4. Borrar datos de navegación
5. Borrar datos



6- Asegurar control de acceso a aplicaciones

Colocar PIN de acceso a aplicaciones con la cual manejes información importante. Telegram cuenta con un sistema de seguridad para bloquear la aplicación con un código pin.

1. Acceder a Telegram
2. Ajustes
3. Privacidad y Seguridad
4. Código de acceso



7- Si es información sensible NO uses SMS ni llamadas convencionales

Utiliza algún programa con llamadas por internet para comunicarte si es información sensible, los medios convencionales son transparentes a cualquiera que quiera verlos.

8- Marcar físicamente -dibujar en- las tarjetas

Hacele una marca la SIM, tarjeta adicional de memoria, batería y teléfono con algo único y no rápidamente perceptible para un extraño.

Pone una cinta adhesiva sobre las juntas del teléfono te ayudará a identificar fácilmente si alguno de estos objetos han sido manipulados o remplazados.

9- No accedas a enlaces o archivos poco confiables que te envíen tus contactos.

Es la principal forma de instalación de malware (software malicioso)

10. Desactivar la ubicación, excepto cuando usemos alguna aplicación de mapas.

De esta forma, aplicaciones como twitter, facebook y google no tendran acceso a nuestra ubicación exacta innecesariamente.

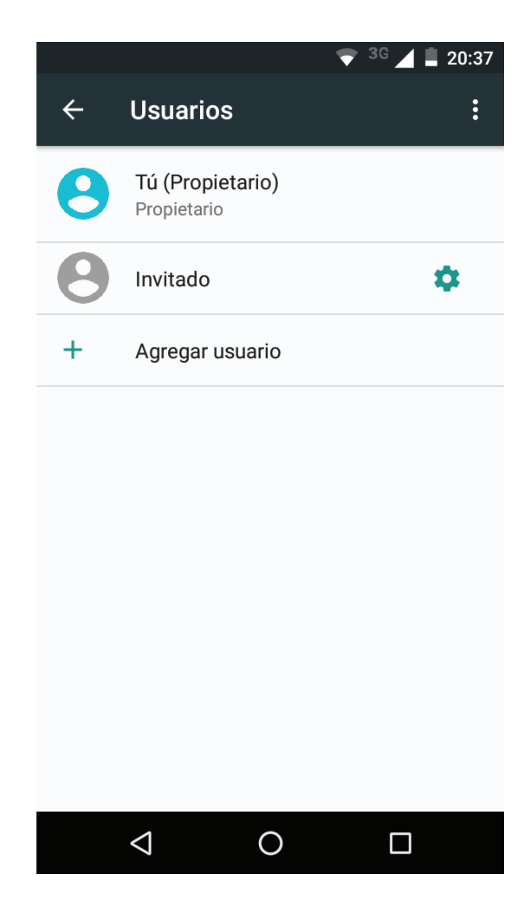
11- Usuario Invitado

Consiste en desvincular tu cuenta del teléfono eligiendo un perfil de usuario diferente al que usamos, Este perfil de usuario invitadx tiene una configuración por defecto o sea una configuración de fabrica.

Es de gran utilidad cuando nos requisan el celular y nos piden acceder al mismo. Si accedemos a un perfil de invitadx no van a encontrar nuestra información personal. Por ende, sugerimos que crear algunos datos ficticios y creibles dentro de este perfil.

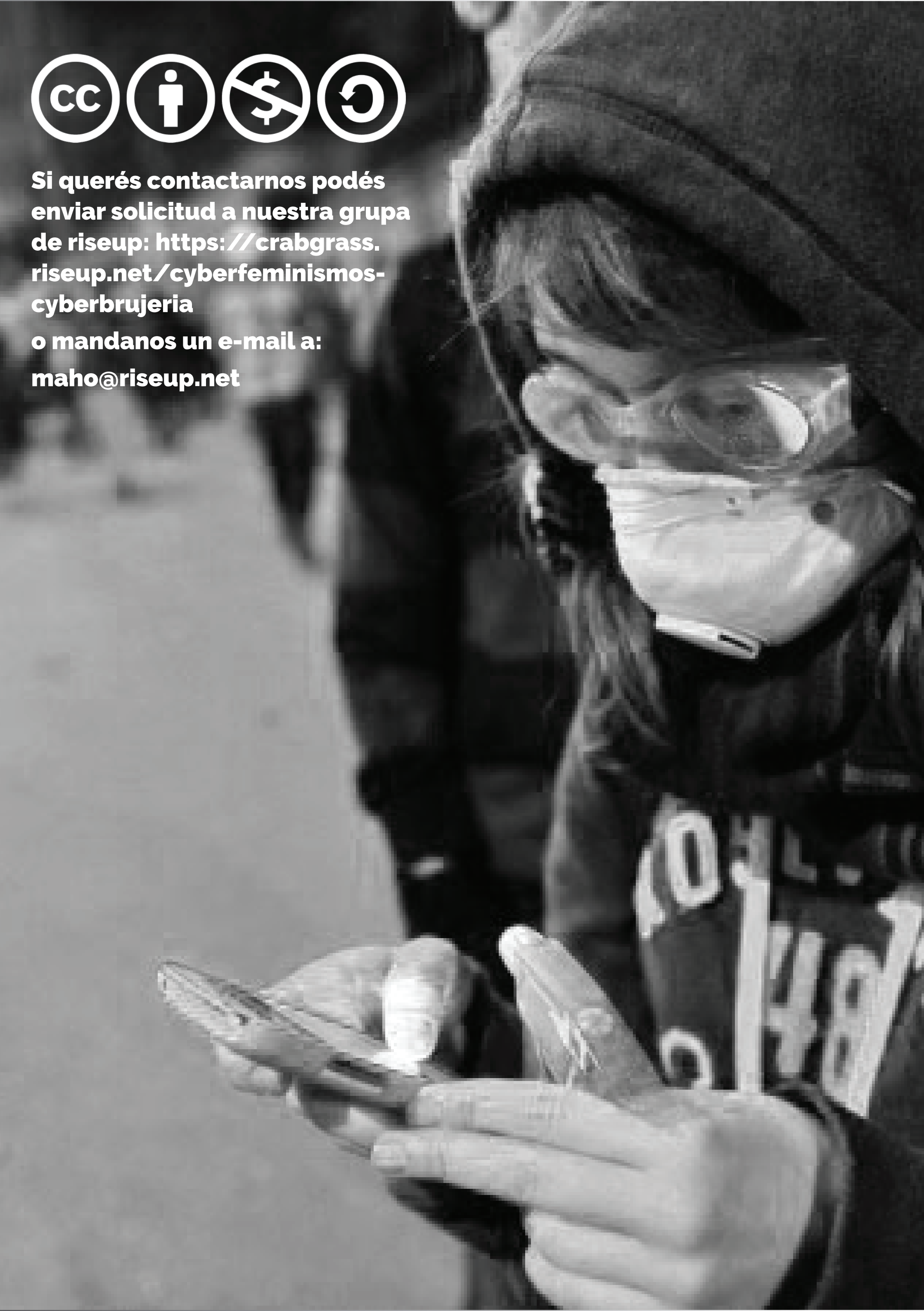
¿Cómo hacerlo?

1. Configuración o Ajustes
2. Usuarios
3. Invitado



Contenido

Info de contacto en la contratapa



Si querés contactarnos podés enviar solicitud a nuestra grupa de riseup: https://crabgrass.riseup.net/cyberfeminismos-cyberbrujeria

o mandanos un e-mail a:

maho@riseup.net